Argonne NATIONAL LABORATORY

… for a brighter future

U.S. Department of Energy

UChicago ▶ Argonne LLC

Office of Science U.S. DEPARTMENT OF ENERGY

A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC

# PSS Generation 1 Upgrade

***Presenter*** *Greg Markovich*

*Safety Interlocks Group Leader*

***Date*** *12/3/07*

# PSS Generation 1 Upgrade

**Reason for Upgrade:**

- Obsolescence of PSS GE Processor and support software
- DIW Monitoring (LOVE controller failures)
- Reorganization combined ACIS and PSS groups
  - *ACIS people saw how PSS was programmed*
  - *PSS people saw how ACIS was programmed*
  - *Both systems safe but functions performed differently*
    - ACIS uses 2 AB PLC's
    - PSS uses AB and GE PLC
    - ACIS Built-in Testability
- Opportunity for Self Assessment
  - Implement the best from PSS & ACIS and current industry safety instrumented systems (SIS)
- To Implement findings from the G3 review

# PSS Generation 1 Upgrade

**The Process:**

- Internal review involved the whole group
- Reviewed SAD
- Reviewed DOE Orders
- Reviewed PLC code for compliance
- Design by committee
- Took over 1 year to get to this stage

- APS review (RSPPC, BSDRSC and Division Mgmt) held 11/29/2007

# PSS Generation 1 Upgrade

**Key changes to PSS G1 System:**

- ***Hardware*** –
  - Replace existing obsolete PSS GE hardware with GE Fanuc PAC-70 rack, power supply and processor.
  - Replace problematic DIW LOVE controllers with PLC analog input modules.
  - APS enable key change (mechanical latching)
  - Active / Stand By button and LED removal
  - Validations to use Touch Panels instead of Windows 98 Laptops running DOS based applications
  - Clock sync signal sent from EPICS

# PSS Generation 1 Upgrade

**Key changes to PSS G1 System:**

- ***Software/Functional***
  - Chain B to be programmed in ladder logic (i.e. ACIS, PSS G3, & PSS G1-ChainA)
  - Latch PSS Chain B faults
  - Cross trip between chains A and B
  - Provide additional coding structure and standardization
  - Create more specific faults (categorize faults & trips)
  - PS1 to be used as a backup to PS2 (taking safety credit)
  - EPICS screens to be completely revamped
  - Search and Secure to Chain B (edge trigger)
    - *Makes Chain B independently require a re-search from Chain A*
  - Doors to unlock when Global Off-Line after a fault

# PSS Generation 1 Upgrade

**Key Changes to PSS G1 System:**

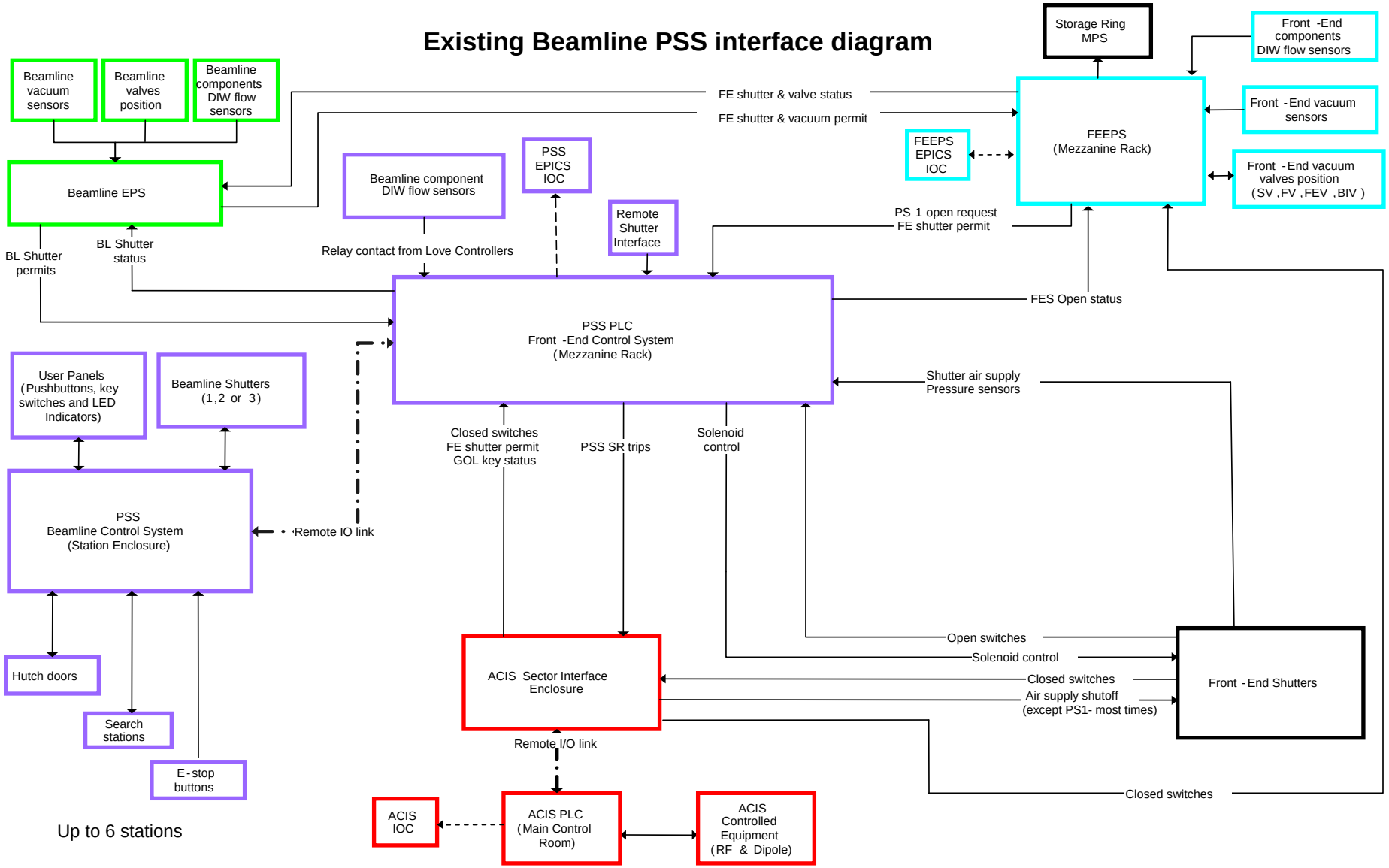
- ***Documentation***
  - SAD – Active/Stand By, Fault/Trip, etc.
  - User Requirements – Active/Stand By, Fault/Trip, etc.
  - Requirements Specification – Add hardware and software changes
  - Validation Procedures – Build test cases from Requirements Spec. Logic and add Touch Panel interface
  - PSS Drawings – Reflect hardware changes

# PSS Generation 1 Upgrade

## Overview of Changes to PSS G1 System:

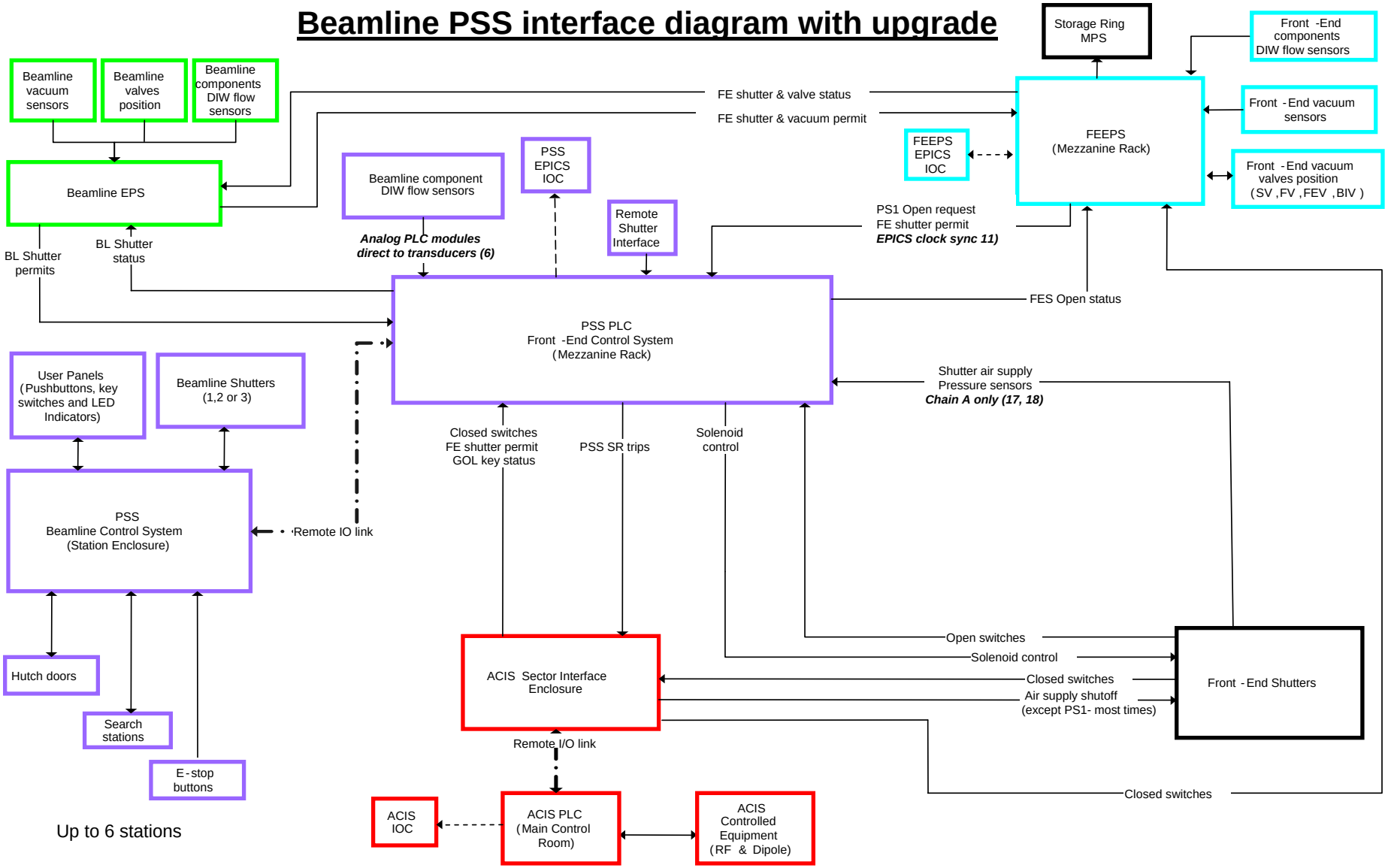
| PSS Features | Generation-1 Existing | Generation-1 Upgrade |
|---|---|---|
| 1. Replace Chain B Processor/Rack | State Logic | Ladder Logic |
| 2. Fault and Trip latching | Chain-A | Chain A & B |
| 3. Categories of Resets called Faults, Trips & Warnings | No | Yes |
| 4. PS1 permit | Chain -A | Chains A & B |
| 5. Search & Secure Chain B | Chain-A to B Level | Chain-A to B Edge |
| 6. PSS component DIW cooling flow | Discrete PLC Inputs (Love) | Analog PLC Inputs |
| 7. Cross Trip function between chains A and B | No | Yes |
| 8. Watch dog timer inhibits for testing | No | Yes |
| 9. Cross trip inhibits to test chain independence | No | Yes |
| 10. Validation Hardware | PC's (laptop) | Touch panel |
| 11. EPICS time sync for chains A and B | No | Yes |
| 12. User Key | Chain-A & B | Chain-A (S&S not required) |
| 13. ACIS trip test | No | Chains A & B |
| 14. EPICS PSS Interface | Read Only Chain A & B | Read Only Chain A & B |
| 15. Active/Stand By | Chain A | No |
| 16. APS Enable Key | Chain A & B (software latch) | Chain A & B (hardware latch) |
| 17. < 3PSI Air | Chain A & B (Fault) | Chain A (Warning) |
| 18. >60PSI Air | Chain A & B (Fault) | Chain A (Warning) |

# PSS Generation 1 Upgrade



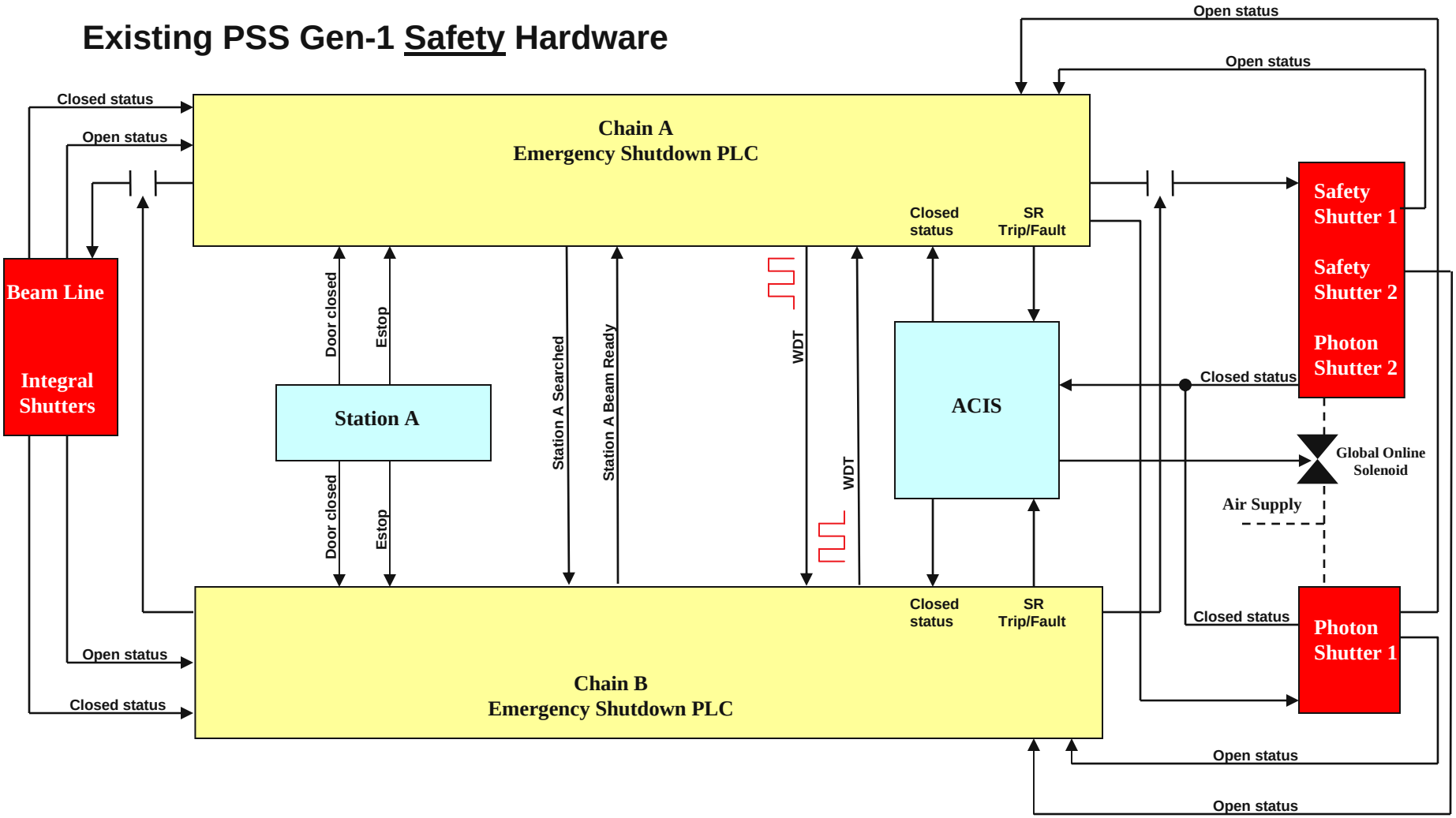
# PSS Generation 1 Upgrade

## Beamline PSS interface diagram with upgrade



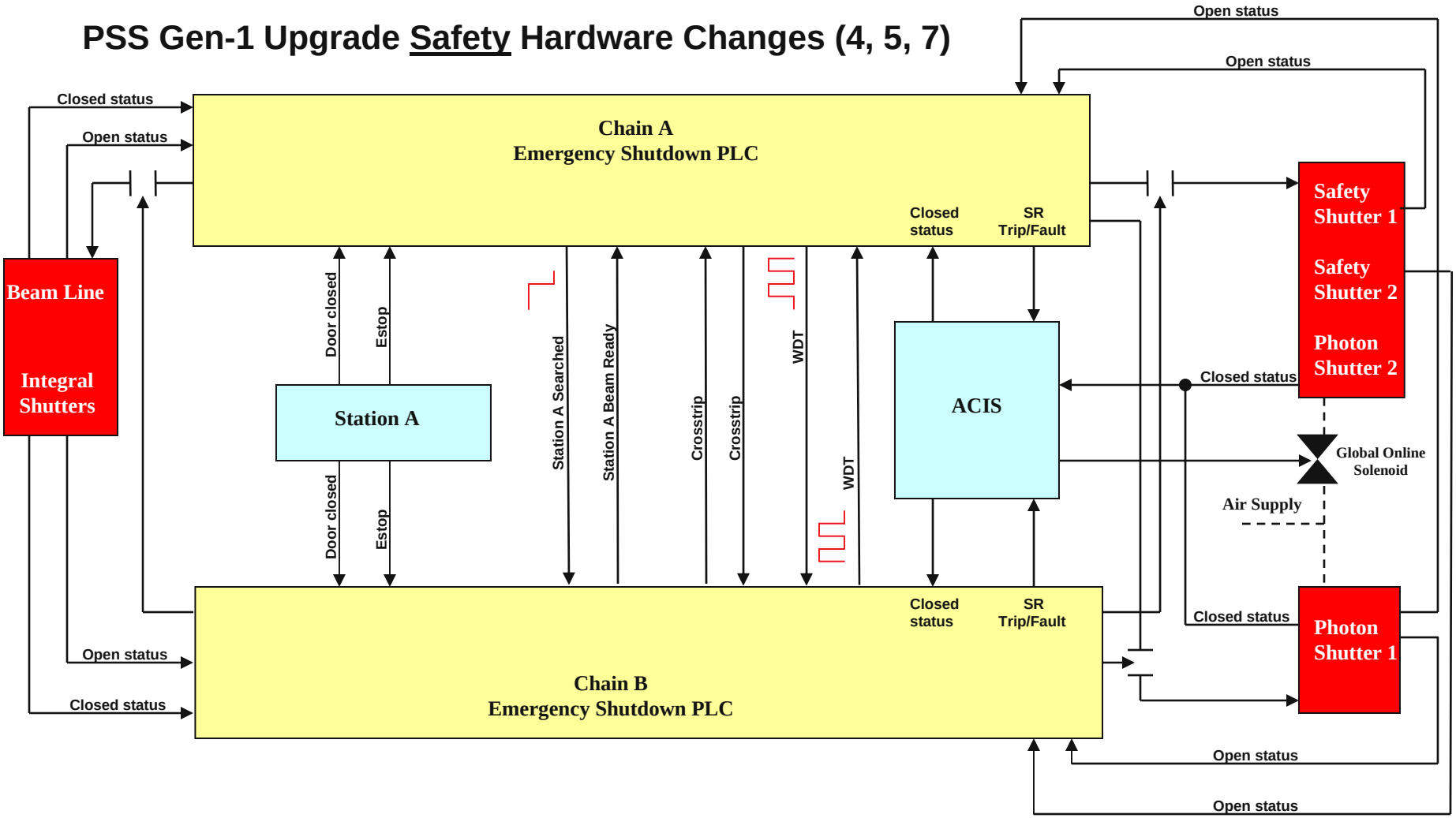
# PSS Generation 1 Upgrade

## Existing PSS Gen-1 Safety Hardware



# PSS Generation 1 Upgrade

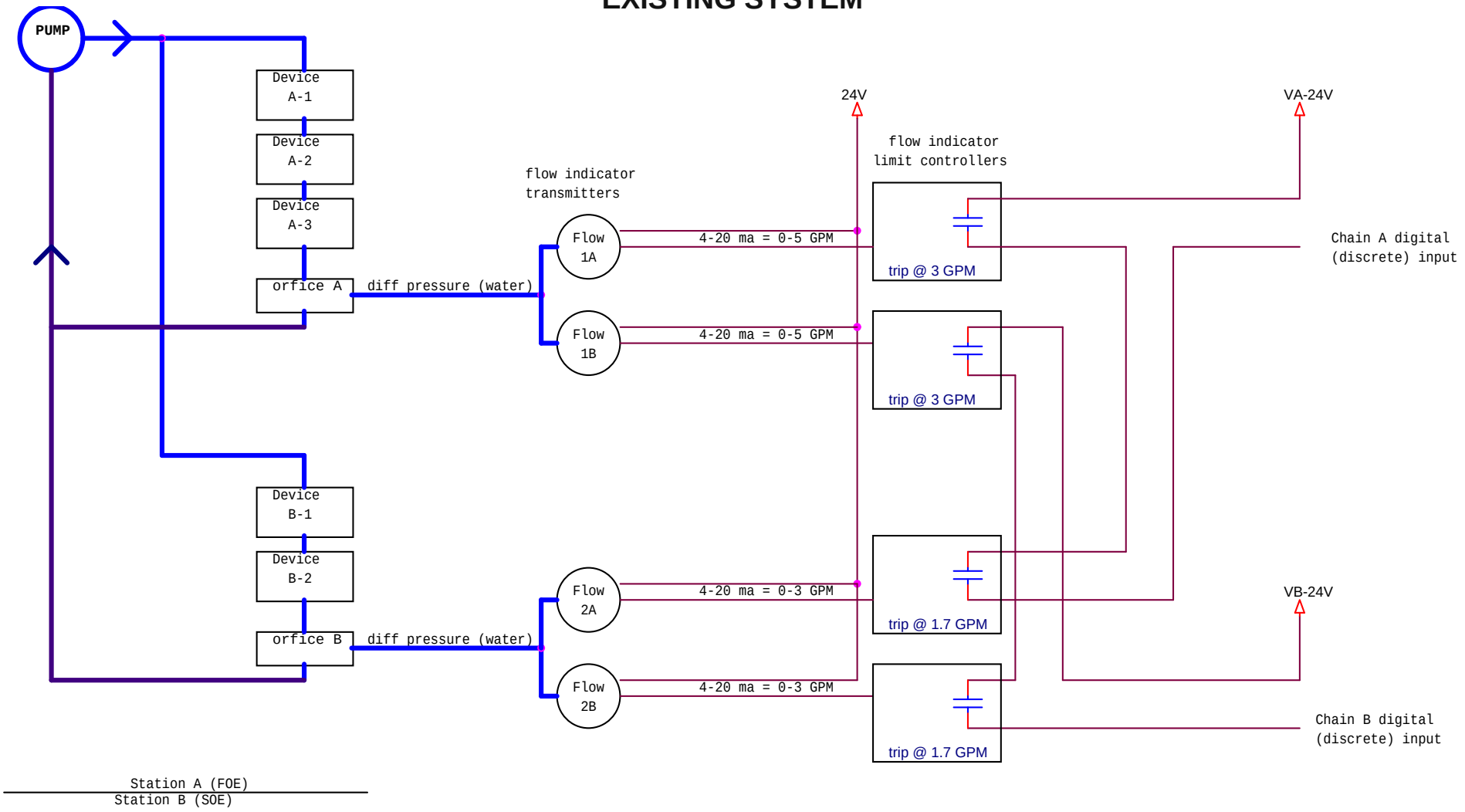
## PSS Gen-1 Upgrade Safety Hardware Changes (4, 5, 7)



# PSS Generation 1 Upgrade

**DIW flow indicator limit controllers (i.e. Love Controllers) for PSS critical beamline cooling flow**

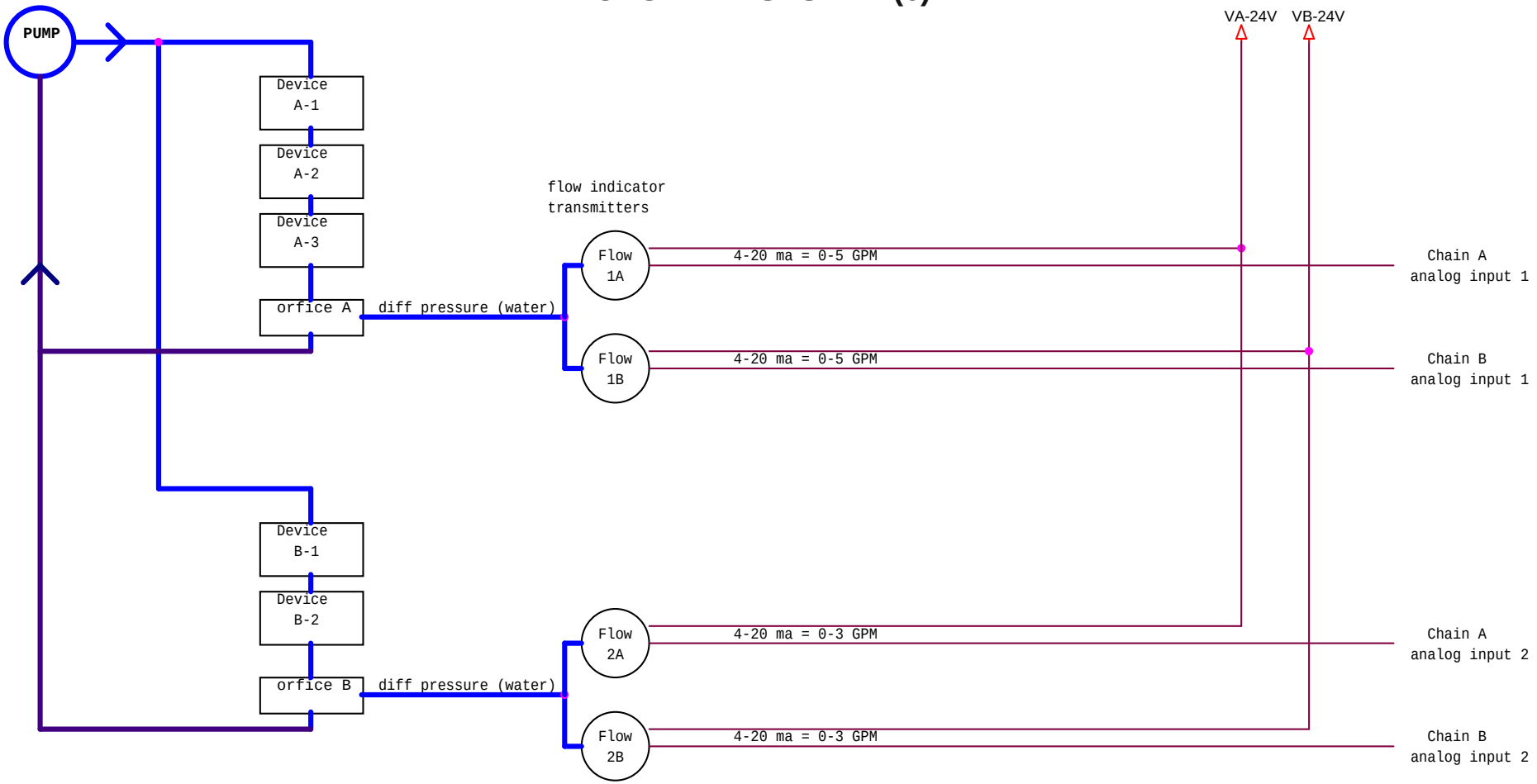
**EXISTING SYSTEM**



# PSS Generation 1 Upgrade

**DIW flow indicator transmitters into PSS PLCs analog inputs for PSS critical beamline cooling flow**

**UPGRADE SYSTEM (6)**




Station A (FOE)
Station B (SOE)

# PSS Generation 1 Upgrade

**Conclusions**

- PSS G1 Upgrade Project Functional Changes Reviewed:
  - RSPPC Waiting for Safety Approval
  - BSDRSC Waiting for Safety Approval
  - DIVISION Waiting for Project Review Approval
- Proposed Implementation Plan
  - Install PSS G1 Upgrade Design at 6BM (In process)
  - Use 6BM Test Bed for ~ 1-2 months of **Non-Beam** Operation/Testing (DIW)
  - Present Operational Results at Readiness Review ~03/08
  - After RR Approval Install first Upgraded system during May08 Shutdown.
  - Proceed to install Upgraded Systems at ~3 per Shutdown/~9 per year.

# PSS Generation 1 Upgrade

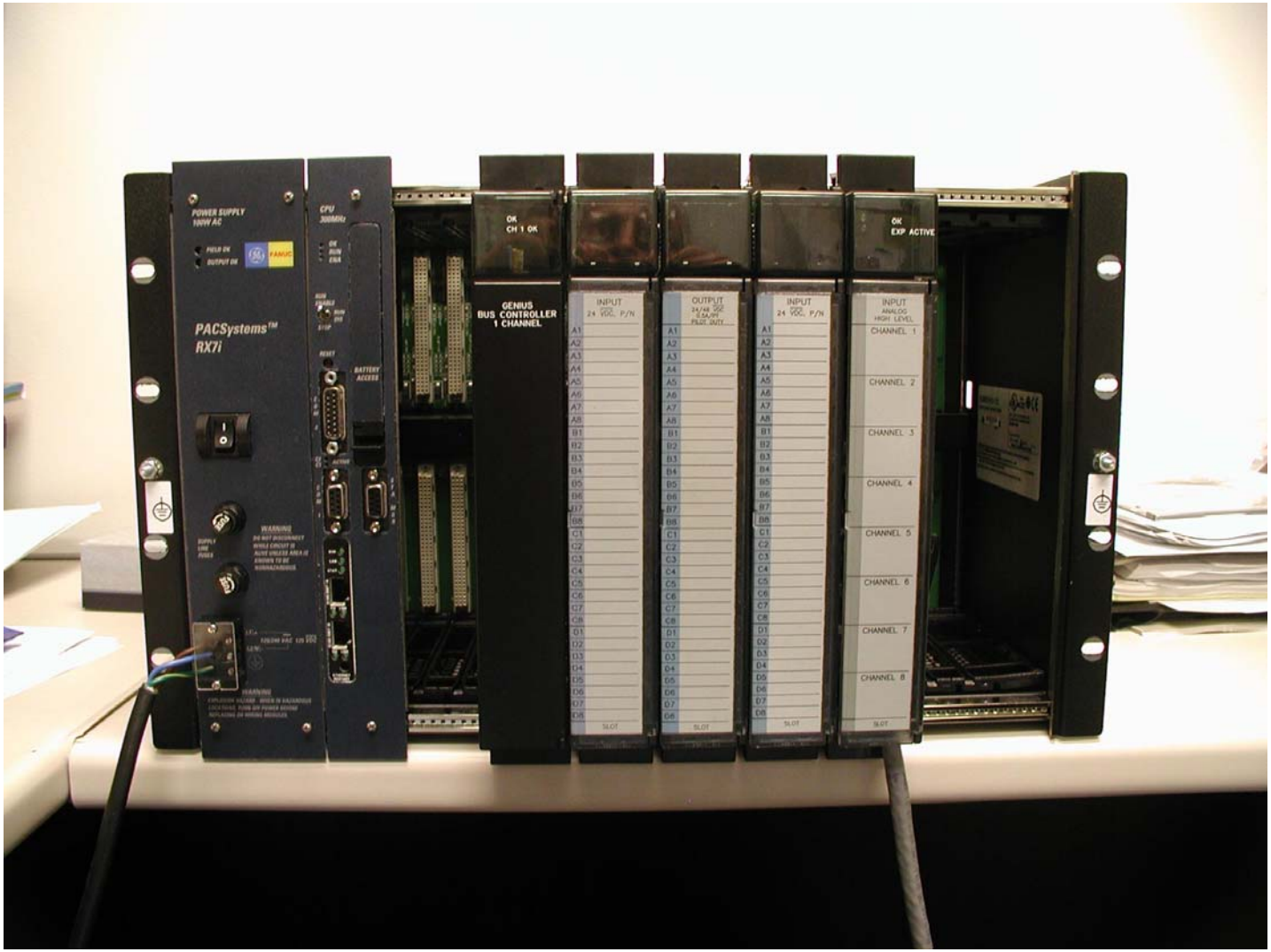
THE FOLLOWING SLIDES ARE FROM THE REVIEW AND ARE FOR

**REFERENCE ONLY**

# Internal APS Safety Review: PSS Generation 1 Upgrade


**PSS Gen-1 Current Chain B Local Chassis Hardware**

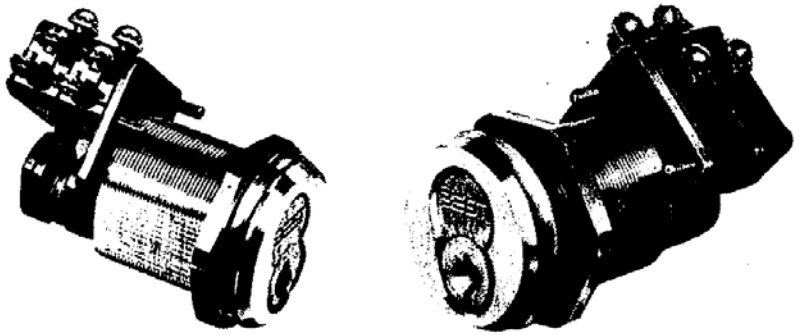
# Internal APS Safety Review: PSS Generation 1 Upgrade

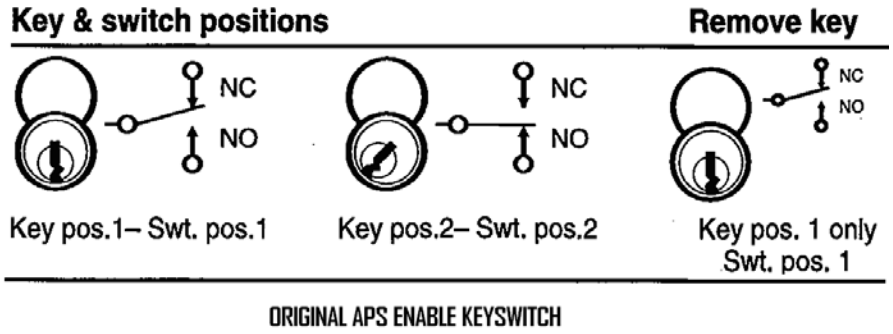



**PSS Gen-1 Upgrade Chain B Local Chassis Hardware (1, 14)**

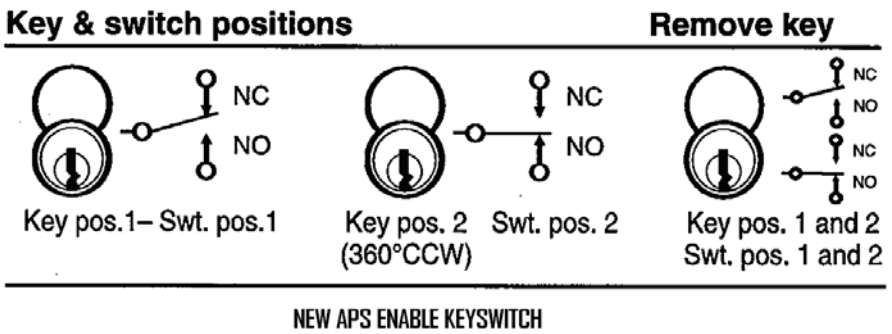
# Internal APS Safety Review: PSS Generation 1 Upgrade

## APS ENABLE Key operation change (16)






ORIGINAL APS ENABLE KEYSWITCH




NEW APS ENABLE KEYSWITCH

# Internal APS Safety Review: PSS Generation 1 Upgrade

**Removing the Active/Standby button function (15)**

# Internal APS Safety Review: PSS Generation 1 Upgrade

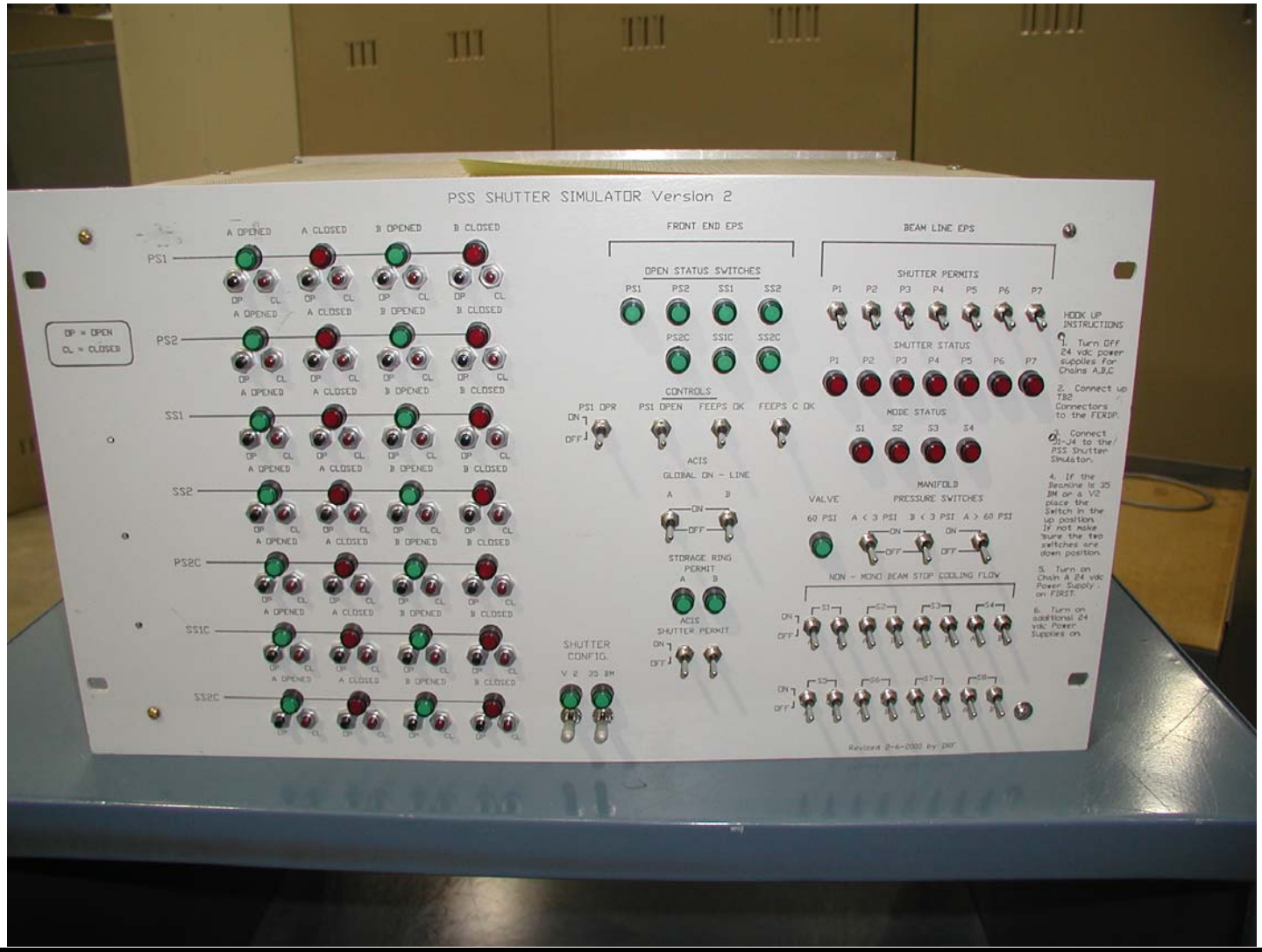
## Restructure Minor and Major Faults to Faults, Trips & Warnings (3)

Original System Panel

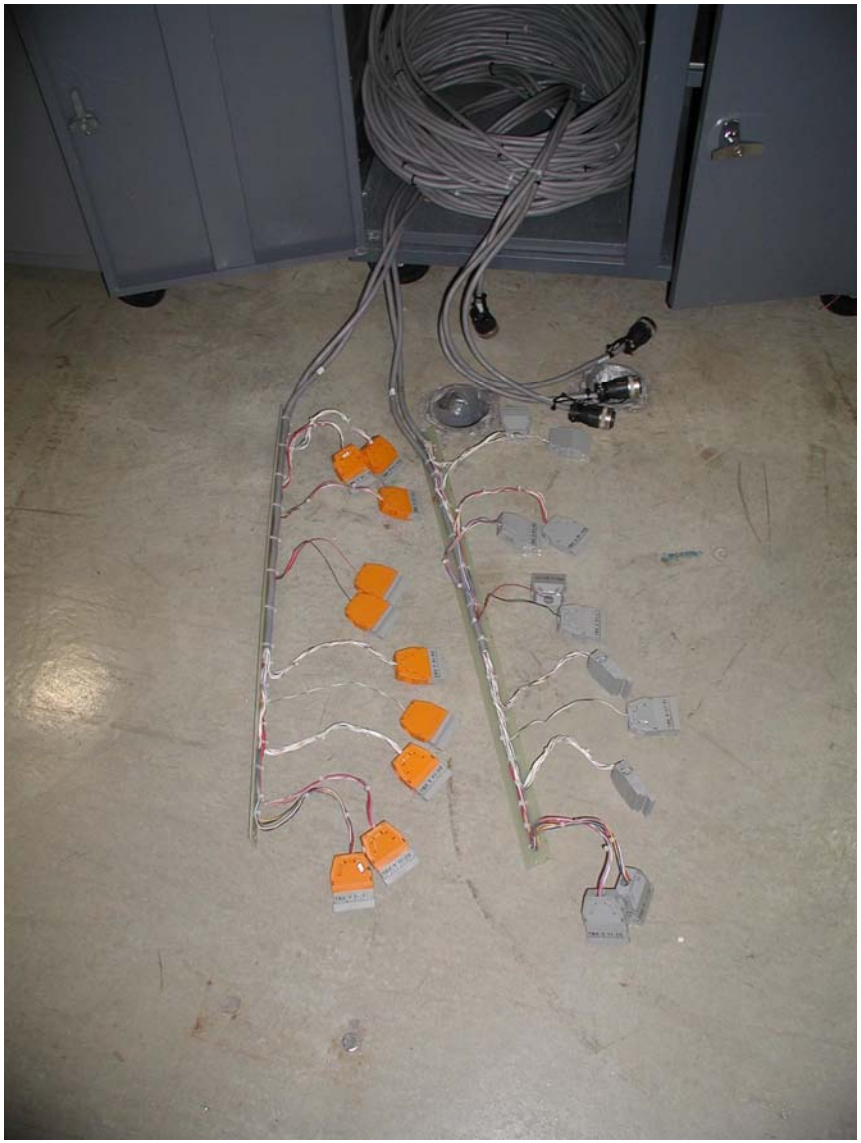

New System Panel

# Internal APS Safety Review: PSS Generation 1 Upgrade

## PSS Gen-1 Validation FES Simulator

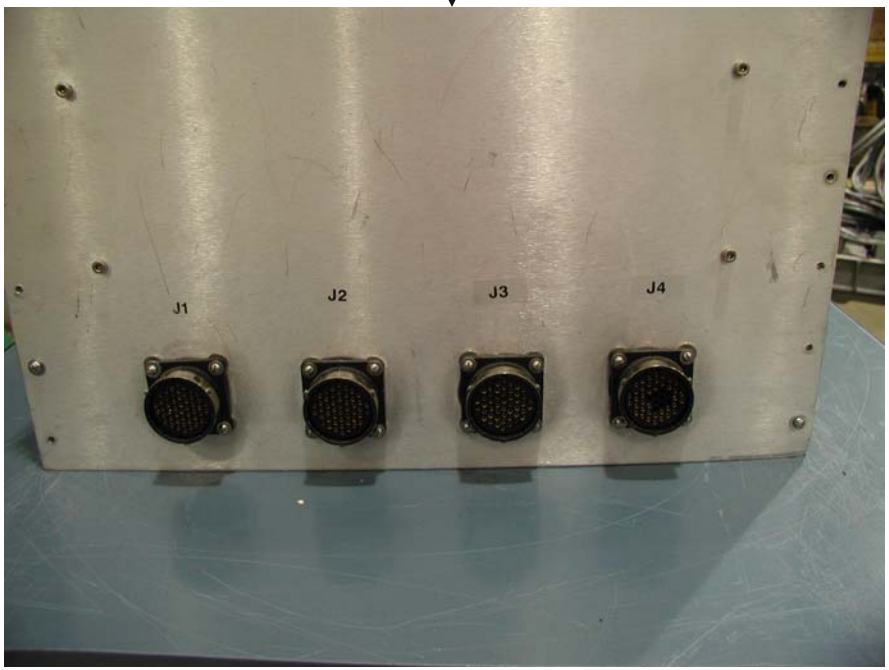


# Internal APS Safety Review: PSS Generation 1 Upgrade

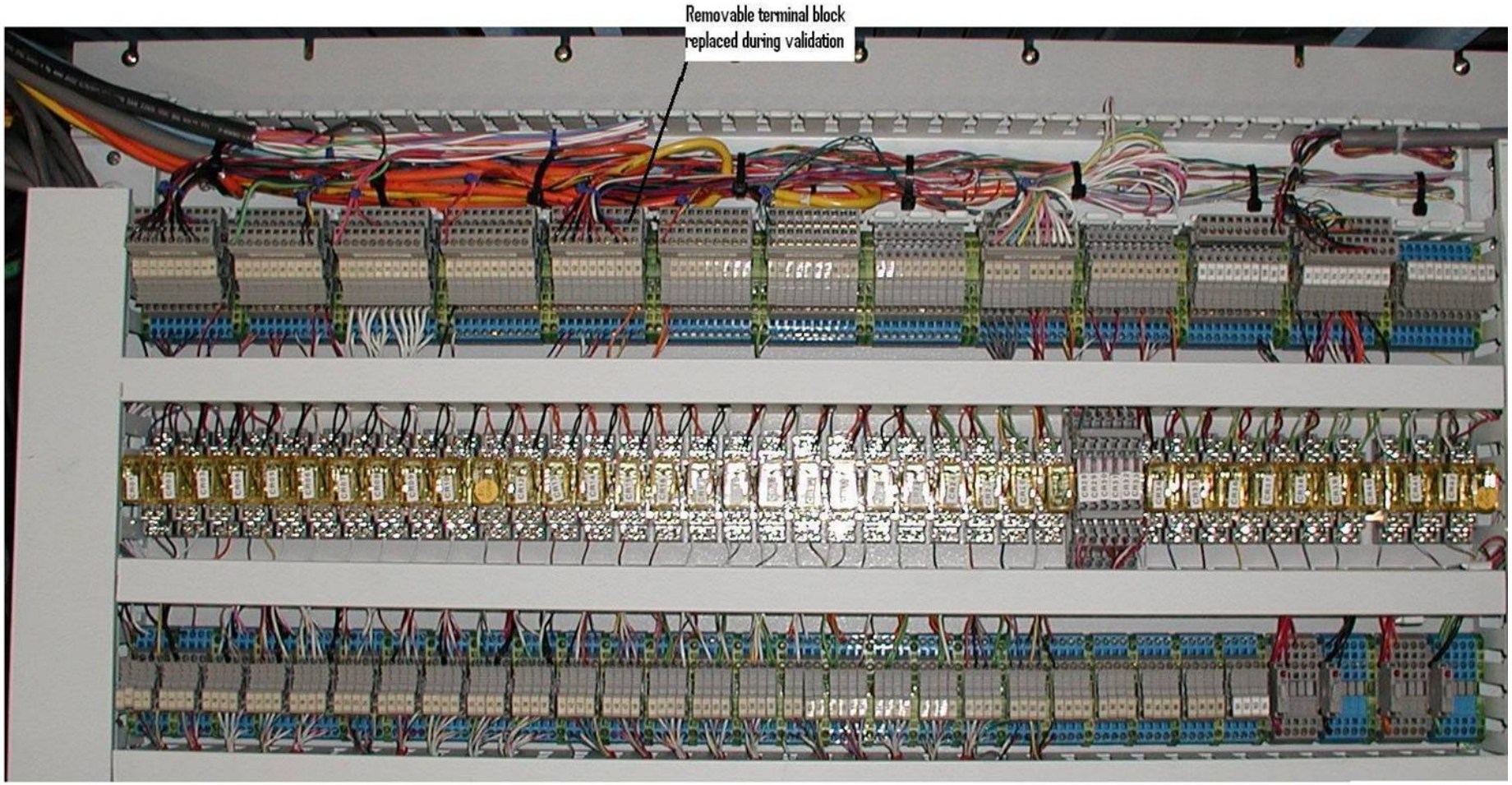


Validation FES Simulator Cables

Validation FES Simulator Rear Panel



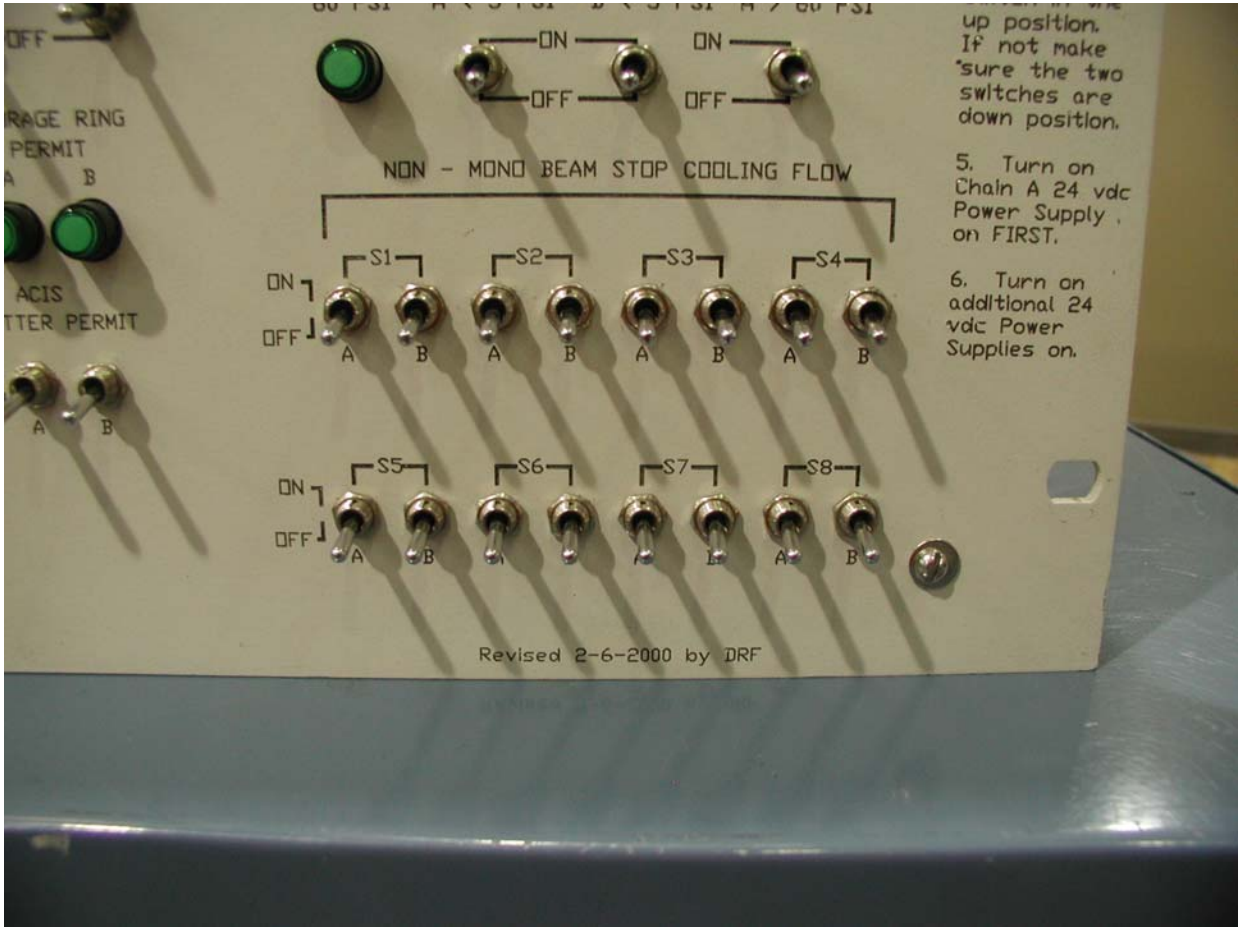
# Internal APS Safety Review: PSS Generation 1 Upgrade




**PSS Gen-1 Front-End Relay Distribution Panel**

# Internal APS Safety Review: PSS Generation 1 Upgrade

**No hardware changes, only reallocation of existing signals**



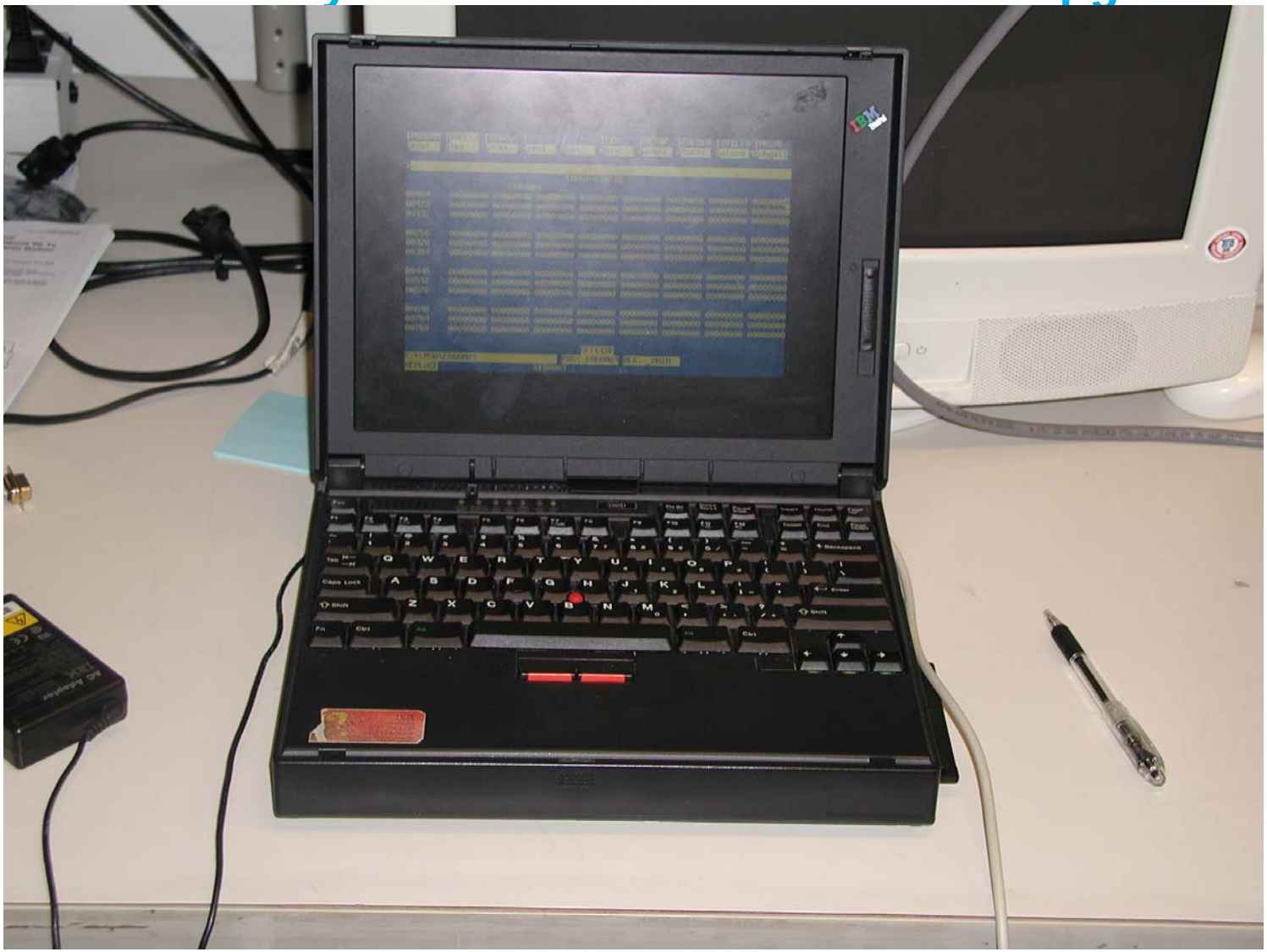

**Beamstop cooling flows S1-S8 become ACIS Trip tests, WDT inhibits, Cross Trip inhibits & Output disable (8, 9, 13)**

# Internal APS Safety Review: PSS Generation 1 Upgrade

## What is the Output Disable input from the PSS Shutter Simulator?

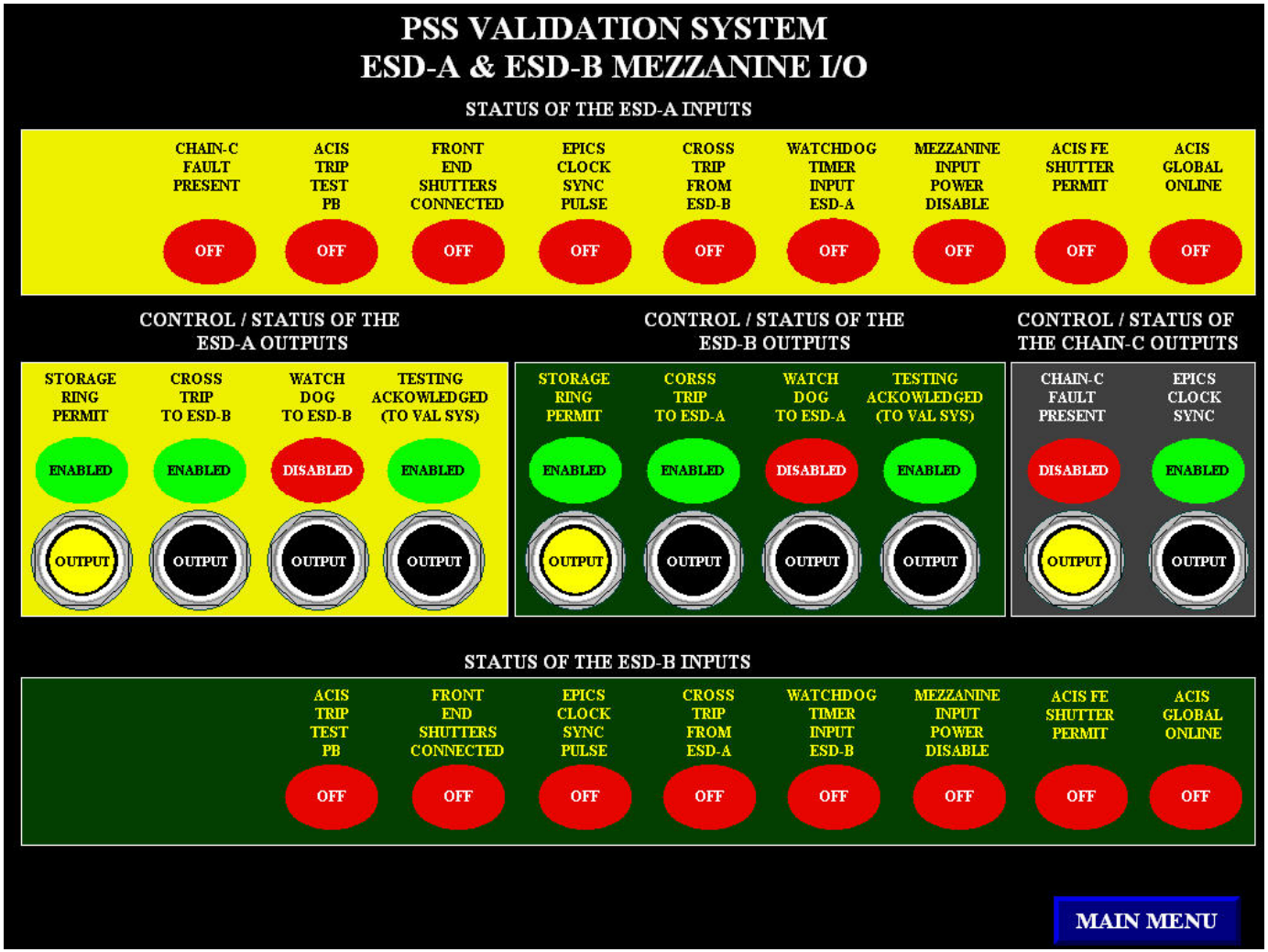
- To leave the ESD PLC code running, but stop the outputs from being turned ON, only when this test signal called “outputs disable” is present.
- This allows an temporary external HMI the ability to turn ON and OFF any PLC output to test the field wiring from that PLC module to the field device (e.g. Strobe Light or Shutter Solenoid).
- PLC input field wiring can be tested this way as well, by actuating the field device and watching the HMI indicate which PLC input changed.
- All this is done today by connecting a laptop to the ESD PLC and using the PLC vendors proprietary software development programs (some DOS and some Windows based) to monitor inputs and force outputs.

# Internal APS Safety Review: PSS Generation 1 Upgrade



**DOS based GE validation laptop**

# Internal APS Safety Review: PSS Generation 1 Upgrade




**New HMI based I/O check with programmable touch screen (10)**

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- **Add latching of the PSS Chain B faults/trips. (2)**
  - **In the current implementation, when a fault/trip is detected, Chain B will pull the appropriate permits, either to remove the Storage Ring Permit to ACIS, thus removing beam from the storage ring or closing the shutters thus removing beam from the stations.**
  - **Once the conditions that created the fault/trip are removed, the permits are restored**
    - **The programmed response to the fault/trip often removed the conditions that created the fault/trip (e.g. door open with beam in station, this trip would remove the storage ring permit and close all of the shutters, thus removing the conditions that created the trip and reissuing the permits that it once removed without requiring a reset).**
    - **While this had no safety impact, it did make determining the cause for the beam removal difficult to determine**
  - **In the planned implementation the fault/trip will be latched and will hold the permits off until reset**
    - **This will allow problems to be diagnosed faster and more efficiently.**

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- The SI group internal review process resulted in an analysis of the current fault structure (3)
  - Currently, all system responses are called faults and are grouped based on their effect
    - Major – remove the storage ring permit to ACIS
    - Serious – remove permits to all shutters and lock all station doors
    - Minor – remove permits to all shutters
  - This makes no differentiation between when the system is doing what it is designed to do and when it has detected an internal problem (i.e. hardware failure)

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- The new system responses will be classified by their cause
  - Trip – System has responded as expected to an attempt to breach the safety envelope
    - e.g. Door opened while beam active
  - Fault – System has detected an internal inconsistency that may cause the PSS to be unable to perform in its required safety function (e.g. hardware fault)
    - e.g. Shutter switches show both opened and closed at the same time
  - Warning – Non Safety related issue
    - e.g. DIW flow below set point while station not APS Enabled
- This has no effect on the safety of the system, but helps to identify when the system needs repair, as opposed to an investigation of a possible attempt to breach the safety envelope

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- **Photon Shutter 1 permit will be added to Chain B (4)**
  - **Currently, both Chains A & B monitor and take backup radiation safety credit for Photon Shutter 1**
    - **Backup radiation credit means if Photon Shutter 2 fails to close, Photon Shutter 1 can be closed. Therefore, when access to the beamline is made, the beam is considered blocked and the storage ring does not need to be dumped**
    - **Currently, only Chain A can close Photon Shutter 1 when Photon Shutter 2 fails**
  - **Currently, ACIS does not take any radiation safety credit for Photon Shutter 1**
    - **ACIS only monitors Photon Shutter 2**
    - **Should the beamline be taken "global off-line" while Photon Shutter 1 is acting as backup, the storage ring will be dumped**
  - **In the new implementation, both Chains A & B will be able to close Photon Shutter 1 when they detect a failure of Photon Shutter 2**
  - **ACIS will be modified to also monitor Photon Shutter 1, if approved**

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- The placement of the search function was re-examined (5)
  - Currently, it is only in Chain A
    - Chain B fully trusts the search status sent from Chain A
  - ACIS is a hybrid, the search function is in both chains, however the inputs are passed from Chain A to Chain B
  - The decision was made to leave the search function in only Chain A, but to make Chain B's acceptance of it more "intelligent"
    - Chain B will only consider a station searched when it receives a false to true transition on the "station searched from Chain A" input while it senses all doors closed and all crash buttons pulled out. The searched status will be lost if Chain B senses any door open or any crash button pressed
    - Since the loss of the search status will remove Chain B's permits, the shutters can not be reopened without the station being researched and the operator will be warned of this condition by the Chain B warning indicator. Further details can be found on appropriate EPICS display.

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- With the addition of Analog modules to replace the “Love” controllers (6)
  - Additional programming is required to initialize, and set the scaling and low-flow trip points for each analog channel
  - Additional module error checking will be programmed into each ESD PLC
  - A method to change the trip points with portable HMI is being developed (this method will not require PLC code validation process following the change)
  - The validation process will need to check both the functionality and the scaling of each channel

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- Trips or Faults that result in removing the storage ring permit to ACIS will also create cross trip to the other chain. (7)
  - This provides an alternate electrical path to remove the beam in the storage ring through the other chain.
- Considerable effort has been made to prevent secondary trips/faults
  - i.e. trips/faults that occur after the original trip/fault or as a side effect of its actions, some examples are:
    - A “crash button pressed while beam active” would also create a “Crash button pressed while searched” trip
    - Since the first drops the storage ring permit and closes all shutters, there is no reason to generate the second which just closes all shutters
  - Does not change the safety of the system, but makes it easier to troubleshoot
  - Trips/faults only block other trips/faults of same or lesser consequence

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- Other misc changes
  - Added a Watchdog Timer Disable input (allows testing without unplugging relay) (8)
    - Should this input fail, the other chain would render beamline safe
  - Added a Cross Trip Inhibit input (allows for chain independence testing) (9)
    - Should this input fail, PSS would only lose a redundant path to remove the Storage Ring Permit
    - Redundant path only comes into play in case of a double failure
    - Therefore, this scenario would require a triple failure before loss of the added redundancy.
  - Added a EPICS Time Sync input (keeps all time stamps in sync) (11)
    - Only used to synchronize diagnostic time stamps, no safety effect if this input fails.

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- **Other misc changes (cont.)**
  - User key in the enable position is no longer required for search and secure(12)
    - Directly inhibits shutter open operation, instead of indirectly through search and secure function
    - User key now part of control logic, not permit logic
  - Added an ACIS Trip Test input (allows testing without unplugging relay) (13)
    - Should this input fail, it would force removal of the Storage Ring Permit
    - While this is a nuisance, it is still fail safe.

# Internal APS Safety Review: PSS Generation 1 Upgrade

## Software/Functional Proposed Changes to PSS G1 System:

- Other misc changes (cont.)
  - <3psi shutter pneumatic cylinder pressure now only used to produce an operational warning (17)
  - >60psi shutter pneumatic cylinder pressure now only disables the opening of shutters (i.e. removes permit and indicates warnings) (18)
    - Will no longer force the shutters to close if lost
    - If pressure is adequate to hold shutters open they will stay open
    - Only if shutter open switch is un-activated due to inadequate air pressure does the system respond (no switch fault)
  - Added an Output Inhibit input (allows I/O testing through an HMI)
    - Should this input fail, other chain would sense loss of Watchdog
  - Chain B now programmed in ladder logic, not in state logic (1)
    - Both ESD PLCs using ladder logic programming language was approved in Gen 3 PSS review in 2004